COSE Additional Algorithms

Jim Schaad

August Cellars

What algorithms to include

- What algorithms needed not in the base document?
- Current draft has RSA-OAEP and RSA-PSS
  - No additional CEK, KEK, Key Wrap, Key Agree algorithms
- Current draft has some cruft left over from the history of how the document was created
  - Addition sections
  - CFRG cruft

Inclusion Criteria

- What is the criteria that should be used for adoption of algorithms?
  - Is the primary focus of COSE IoT or do we have non-IoT use cases that are well understood?
  - Will IoT be expected to adopt the algorithm?
    - For IoT – RSA message size is a potential problem. Going from 512-bits to 2048-bits is an issue.
  - Security Analysis/Proofs – What is the minimum acceptable level?
  - What should be the current implementation level for the additional algorithms?

Way Forward and Questions

- Should we publish this draft at this time or wait and see if there is a need for additional algorithms not currently defined
- Should this draft be done in here, in CRUDLE or as an Independent submission